

1 WE CLAIM:

1 1. A secure disk drive comprising:  
2     (a) a disk for storing data;  
3     (b) an input for receiving an encrypted message from a client disk drive, the encrypted  
4         message comprising ciphertext data and a client drive ID identifying the client disk  
5         drive;  
6     (c) a secure drive key;  
7     (d) an internal drive ID;  
8     (e) a key generator for generating a client drive key based on the client drive ID and the  
9         secure drive key, and an internal drive key based on the internal drive ID and the  
10        secure drive key;  
11     (f) an authenticator for verifying the authenticity of the encrypted message and  
12         generating an enable signal, the authenticator responsive to the encrypted message  
13         and the client drive key;  
14     (g) a data processor comprising:  
15         a message input for receiving the encrypted message from the client disk drive;  
16         a data output for outputting the ciphertext data to be written to the disk;  
17         an enable input for receiving the enable signal for enabling the data processor;  
18         a key input for receiving the internal drive key, the internal drive key for use in  
19             generating a message authentication code; and  
20             a reply output for outputting reply data, the reply data comprising the message  
21                 authentication code; and  
22     (h) an output for outputting a reply to the client disk drive, the reply comprising the reply  
23         data and the internal drive ID.

1 2. The secure disk drive of claim 1, wherein the secure drive key is immutable.

- 1    3.    The secure disk drive of claim 1, wherein the secure drive key is mutable.
- 1    4.    The secure disk drive of claim 1, wherein the authenticator comprises a means for  
2       verifying the access rights of the client drive ID.
- 1    5.    The secure disk drive of claim 1, wherein the secure drive key comprises tamper resistant  
2       circuitry.
- 1    6.    The secure disk drive of claim 1, wherein the key generator comprises tamper resistant  
2       circuitry.
- 1    7.    The secure disk drive as recited in claim 1, wherein the authenticator comprises tamper  
2       resistant circuitry.
- 1    8.    The secure disk drive as recited in claim 1, wherein the data processor further comprises  
2       cryptographic facilities.

1    9. A secure disk drive comprising:

2        (a) a disk for storing data;

3        (b) an input for receiving an encrypted message from a client disk drive, the encrypted

4              message comprising ciphertext data and a client drive ID identifying the client disk

5              drive;

6        (c) a secure drive key;

7        (d) an internal drive ID;

8        (e) a key generator for generating a client drive key based on the client drive ID and the

9              secure drive key, and an internal drive key based on the internal drive ID and the

10             secure drive key;

11       (f) an authenticator for verifying the authenticity of the encrypted message and

12              generating an enable signal, the authenticator responsive to the encrypted message

13              and the client drive key;

14       (g) a data processor comprising:

15              a message input for receiving the encrypted message from the client secure disk drive;

16              a data input for receiving ciphertext data read from the disk;

17              an enable input for receiving the enable signal for enabling the data processor;

18              a key input for receiving the internal drive key, the internal drive key for use in

19              generating a message authentication code; and

20              a reply output for outputting reply data, the reply data comprising the ciphertext data

21              read from the disk and the message authentication code; and

22       (h) an output for outputting a reply to the client disk drive, the reply comprising the reply

23              data and the internal drive ID.

1    10. The secure disk drive of claim 9, wherein the secure drive key is immutable.

1    11. The secure disk drive of claim 9, wherein the secure drive key is mutable.

- 1    12. The secure disk drive of claim 9, wherein the authenticator comprises a means for
- 2                 verifying the access rights of the client drive ID.
- 1    13. The secure disk drive of claim 9, wherein the secure drive key comprises tamper resistant
- 2                 circuitry.
- 1    14. The secure disk drive of claim 9, wherein the key generator comprises tamper resistant
- 2                 circuitry.
- 1    15. The secure disk drive as recited in claim 9, wherein the authenticator comprises tamper
- 2                 resistant circuitry.
- 1    16. The secure disk drive as recited in claim 9, wherein the data processor further comprises
- 2                 cryptographic facilities.